

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re: Bardsley et al.

Serial No.: 10/624,158

Filed: July 22, 2003

For: **SYSTEMS, METHODS AND COMPUTER PROGRAM PRODUCTS FOR
ADMINISTRATION OF COMPUTER SECURITY THREAT
COUNTERMEASURES TO A COMPUTER SYSTEM**

Confirmation No.: 7454

Examiner: Roderick Tolentino

Group Art Unit: 2134

Date: August 17, 2007

Mail Stop Appeal-Brief Patents

Commissioner for Patents

P.O. Box 1450

Alexandria, VA 22313-1450

REVISED APPEAL BRIEF

Sir:

Pursuant to 37 C.F.R. § 41.37, Appellants are filing the present *Revised Appeal Brief* in response to the *Notification of Non-Compliant Appeal Brief* mailed August 14, 2007 and in conjunction with the *Notice of Appeal to the Board of Patent Appeals and Interferences* filed on July 16, 2007 in response to the *Final Office Action* ("Final Action") mailed April 27, 2007.

It is not believed that an extension of time and/or additional fee(s) are required, beyond those that may otherwise be provided for in documents accompanying this paper. In the event, however, that an extension of time is necessary to allow consideration of this paper, such an extension is hereby petitioned under 37 C.F.R. § 1.136(a). Any additional fees believed to be due may be charged to Deposit Account No. 09-0457.

Real Party In Interest

The real party in interest is assignee International Business Machines Corporation of Armonk, New York.

Related Appeals and Interferences

The subject matter of the present application is related to U.S. Application Serial No. 10/624,344 (although not by a claim of priority). U.S. Application Serial No. 10/624,344 is currently in prosecution, and Appellants have appealed the rejections of the claims in that

application to the Board of Patent Appeals and Interferences via a *Notice of Appeal* filed December 21, 2006. No decision has yet been rendered in this related appeal as of the filing of the present *Appeal Brief*.

Status of Claims

Claims 1-22 remain pending, each of which is finally rejected. Appellants appeal the final rejection of Claims 1-22. The attached Claims Appendix presents the pending claims as finally rejected in the *Final Action* mailed April 27, 2007.

Status of Amendments

The attached Claims Appendix presents the claims as they currently stand. An *Amendment* was filed in this case on February 22, 2007. This February 22, 2007 *Amendment* was entered. No *Response After Final* was filed.

Summary of Claimed Subject Matter

Independent Claim 1 is directed to a method of administering a countermeasure for a computer security threat to a computer system, such as, for example, the computer systems **T** shown in **FIG. 2** of the present application or one of the target subsystems **540** of **FIGS. 5** and **15** of the present application. As discussed, for example, at page 18, lines 7-9 and page 19, lines 18-25 of the present specification, pursuant to the method of Claim 1, a baseline identification of an operating system type and an operating system release level may be established for the computer system that is compatible with a Threat Management Vector (TMV) (see also Block **1610** of **FIG. 16**). This baseline identification may be performed by a Threat Management Information Base (TMIB) such as, for example, the TMIB **1830** of **FIG. 18** of the present application. One possible embodiment of the data structure of a TMV **400** is illustrated in **FIG. 4** of the present application. As discussed, for example, at page 10, line 14 through page 11, line 1, page 18, lines 9-14, page 19, lines 26-27 and **FIG. 16**, Block **1620** of the present application, a TMV such as, for example, the TMV **400** of **FIG. 4** of the present application may be received by, for example,

the TMV Inductor **1850** of **FIG. 18** of the present application. The TMV **400** may includes a first field **401** that provides identification of an operating system type that is affected by a computer security threat, a second field **402** that provides identification of an operating system release level for the operating system type and a third field **403** that provides identification of a set of possible countermeasures for the operating system type and release level. As discussed, for example, at page 18, lines 22-27, page 19, line 26 through page 20, line 9 and **FIG. 16**, Blocks **1630-1640** of the present application, the countermeasures that are identified in the TMV may then be processed by, for example, Remediation Manager **1870** of **FIG. 18** of the present application, if the TMV identifies the operating system type and operating system release level for the computer system as being affected by the computer security threat.

Independent Claim 11 is directed to a computer system such as, for example, the computer systems **T** shown in **FIG. 2** of the present application or one of the target subsystems **540** of **FIGS. 5** and **15** of the present application. The computer system includes a Threat Management Information Base (TMIB) such as, for example, the TMIB **1830** of **FIG. 18** of the present application. As discussed, for example, at page 18, lines 7-9 and page 19, lines 18-25 of the present specification, the TMIB is configured to establish a baseline identification of an operating system type and an operating system release level may be established for the computer system that is compatible with a Threat Management Vector (TMV) (see also Block **1610** of **FIG. 16**). One possible embodiment of the data structure of a TMV **400** is illustrated in **FIG. 4** of the present application and is discussed at page 10, line 14 through page 11, line 1 of the present application.

The computer system further includes a TMV receiver that is configured to receive a TMV such as, for example, the TMV Inductor **1850** of **FIG. 18** of the present application. (Specification at page 18, lines 9-14, page 19, lines 26-27 and **FIG. 16**, Block **1620**). One possible embodiment of the data structure of a TMV **400** is illustrated in **FIG. 4** of the present application. The TMV **400** may includes a first field **401** that provides identification of an operating system type that is affected by a computer security threat, a second field **402** that

provides identification of an operating system release level for the operating system type and a third field **403** that provides identification of a set of possible countermeasures for the operating system type and release level. (Specification at page 10, line 14 through page 11, line 1). As discussed, for example, at page 18, lines 22-27, page 19, line 26 through page 20, line 9 and **FIG. 16**, Blocks **1630-1640** of the present application, the computer system further includes a remediation manager such as, for example, Remediation Manager **1870** of **FIG. 18** of the present application, that is configured to process countermeasures that are identified in the TMV if the TMV identifies the operating system type and operating system release level for the computer system as being affected by the computer security threat.

Independent Claim 21 is directed to a computer program product that is configured to administer a countermeasure for a computer security threat to a computer system, such as, for example, the computer systems **T** shown in **FIG. 2** of the present application or one of the target subsystems **540** of **FIGS. 5** and **15** of the present application. The computer program product includes a computer useable storage medium having computer-readable code embodied in the medium. (See, e.g., Specification at page 8, line 20 through page 9, line 13). As discussed, for example, at page 18, lines 7-9 and page 19, lines 18-25 of the present specification, the computer readable program code is configured to establish a baseline identification of an operating system type and an operating system release level for the computer system that is compatible with a Threat Management Vector (TMV) (see also Block **1610** of **FIG. 16**). The computer program product further includes computer readable code that is configured to receive the TMV. (Specification at page 18, lines 9-14, page 19, lines 26-27 and **FIG. 16**, Block **1620**). The TMV may, for example, have the data structure of TMV **400** that is illustrated in **FIG. 4** of the present application. Thus, the TMV **400** may include a first field **401** that provides identification of an operating system type that is affected by a computer security threat, a second field **402** that provides identification of an operating system release level for the operating system type and a third field **403** that provides identification of a set of possible countermeasures for the operating system type and release level. (Specification at page 10, line 14 through page 15, line 1). The

computer program product further includes computer readable code that is configured to process countermeasures that are identified in the TMV if the TMV identifies the operating system type and operating system release level for the computer system as being affected by the computer security threat. (Specification at page 18, lines 22-27, page 19, line 26 through page 20, line 9 and **FIG. 16**, Blocks 1630-1640).

Grounds of Rejection to be Reviewed on Appeal

The rejections of Claims 1-22 under 35 U.S.C. § 103(a) as being obvious over U.S. Patent No. 7,073,198 to Flowers et al. ("Flowers") in view of U.S. Patent Publication No. 2004/0006704 to Dahlstrom et al. ("Dahlstrom").

Argument

I. The Rejections of Claims 1-22 Should be Reversed

As noted above, Claims 1-22 stand rejected under 35 U.S.C. § 103(a) as being obvious over Flowers in view of Dahlstrom. Appellants respectfully submit for the reasons presented below that the combination of Flowers and Dahlstrom fails to render any of the pending claims obvious.

A. Independent Claims 1, 11 and 21 are Patentable Over the Cited Art

Independent Claims 1, 11 and 21 are related method, system and computer program product claims. Claim 1, which is representative of all three claims, recites:

1. A method of administering a countermeasure for a computer security threat to a computer system, comprising:

establishing a baseline identification of an operating system type and an operating system release level for the computer system that is compatible with a Threat Management Vector (TMV);

receiving a TMV including therein a first field that provides identification of at least one operating system type that is affected by a computer security threat, a second field that provides identification of an operating system release level for the operating

system type and a third field that provides identification of a set of possible countermeasures for an operating system type and an operating system release level; and processing countermeasures that are identified in the TMV if the TMV identifies the operating system type and operating system release level for the computer system as being affected by the computer security threat.

Appellants respectfully traverse the rejections of Claims 1, 11 and 21 for at least the following two independent reasons.

First, the Final Office Action ("Final Action") cites to paragraph [0006] of Dahlstrom as disclosing the second recitation of Claim 1. (Final Action at 6). This paragraph of Dahlstrom recites:

In one embodiment of the present invention, a method for determining security vulnerabilities is disclosed that includes receiving a profile of one or more products used by an organization, the profile including characteristics of each product. The method further includes comparing the characteristics of each product to a plurality of product records, each product record including one or more security vulnerabilities associated with the product record and one or more fixes associated with each security vulnerability. The method further includes determining at least one security vulnerability of the one or more security vulnerabilities for at least one of the one or more products in response to comparing the characteristics of the at least one of the one or more products to the product record.

Thus, what Dahlstrom teaches is received is "a profile of one or more products used by an organization" where the profile lists characteristics of each product used by the organization. In contrast, Claims 1, 11 and 21 recite "receiving a [Threat Management Vector]" or "TMV", where the TMV contains (1) a field that identifies an operating system that is affected by a computer security threat, (2) a field that identifies an operating system release level and (3) a field that identifies a set of possible countermeasures for the identified operating system/release level. Appellants respectfully submit that the "organization profile" discussed in paragraph [0006] of Dahlstrom does not teach or suggest the Threat Management Vector of Claims 1, 11 and 21, as there is no teaching or suggestion that these product profiles would include (1) fields showing an operating system type and release level that are affected by a specific security threat or (2) a field that identifies a set of possible countermeasures for the identified operating system/release level.

In fact, if the organization submitting such a profile already had information regarding the identified security threats and the appropriate countermeasures thereto, there would be no need for the organization to submit the profile to have the system of Dahlstrom perform a vulnerability assessment thereon. Accordingly, the product profiles of paragraph [0006] of Dahlstrom clearly do not correspond to the TMV recited in Claims 1, 11 and 21.

Appellants acknowledge that the organizational organization profile **72** illustrated in Fig. 4 of Dahlstrom and described at paragraphs [0041]-[0042] of Dahlstrom shows that the profile **72** may include "Product Tracking Information" that includes vulnerability information **428** and fixes for such vulnerabilities **436**. However, Dahlstrom also makes clear that this portion of the organization profile **72** is complied by a tracking system **80** that is part of the system **20** of Dahlstrom, and hence this security vulnerability and vulnerability fix information **428**, **436** is not a "received" part of an organization profile **72**, but instead is information that is tracked and added by the system of Dahlstrom. (*See, e.g.*, Dahlstrom at paragraphs [0032] and [0049]-[0051]). Thus, Dahlstrom makes clear that it is only the "Product List A" of Fig. 4 of Dahlstrom that is received by the system of Dahlstrom, and the remaining information in Fig. 4 is information compiled by the system of Dahlstrom.

In the Response to Arguments section of the Final Action, a new argument is raised as to why Dahlstrom allegedly discloses the second recitation of Claim 1 (as well as the corresponding recitations of Claims 11 and 21). In particular, the Final Action newly cites to paragraphs [0023]-[0026] of Dahlstrom and argues that the "product records" **52** described therein correspond to the TMV recited in Claims 1, 11 and 21. (Final Action at 2). The Final Action further argues that the product records **52** of Dahlstrom must have been "inherently" received from at least one source. (Final Action at 2). However, it is simply not inherent (i.e., necessarily the case) that the product records **52** of Dahlstrom are received from a source. Instead, the security vulnerability database of Dahlstrom could easily comprise an internally generated database of information. Thus, as neither of the cited references disclose "receiving a TMV" as recited in Claims 1, 11 and 21, the rejection of Claims 1, 11 and 21 under 35 U.S.C. § 103 should be reversed.

Second, Appellants respectfully submit that the rejections of Claims 1, 11 and 21 should be reversed because a person of ordinary skill in the art would not have combined Flowers and Dahlstrom in the manner suggested. Flowers discloses a system which sends packets to a remote host and, based on the response to these packets, **determines the operating system, version and patch level** of the remote host, which provide an indication of the vulnerability of the remote host. (Flowers at Col. 4, lines 14-67). In contrast, with the system of Dahlstrom, an organization desiring a security review completes and submits an organizational profile of the "hardware and software products used by the organization." (Dahlstrom at ¶ 0036). As shown in Fig. 4 of Dahlstrom, this organizational profile **includes** operating system, version and patch information. The system of Dahlstrom compares the organizational profile to a securities vulnerability database to identify vulnerabilities associated with the organizations' products. (*Id.*). Thus, Flowers provides a method for **determining** the operating system, version and patch status of a particular remote device, whereas in Dahlstrom this information is directly provided by each organization using the security service. Clearly, one of skill in the art would not have been motivated to incorporate the system of Dahlstrom into the system of Flowers as suggested in the pending rejections, as in the system of Dahlstrom the operating system, version and patch level information are **directly provided by the organization** (along with other information). In other words, since Dahlstrom receives the organizational profile, it makes no sense to run the system of Flowers to try to deduce the operating system, version and patch level information. Accordingly, the rejections of Claims 1, 11 and 21 should be reversed for this additional reason.

B. Claims 2, 8, 12 and 18 are Separately Patentable Over the Cited Art

Claims 2 and 12 depend from Claims 1 and 11, respectively. Claims 8 and 18 depend from Claims 2 and 12, respectively. Accordingly, Claims 2, 8, 12 and 18 are each patentable as depending from a patentable base claim. In addition, Appellants submit that Claims 2 and 12 (and Claims 8 and 18 depending therefrom) are independently patentable over the cited art. In particular, the Final Action states that paragraph [0018] of Dahlstrom discloses "receiving a

TMV history file in response to installation, configuration or maintenance of the computer system" as recited in Claims 2 and 12. However, paragraph [0018] of Dahlstrom says nothing about receiving a TMV history file, and it appears that it was cited against Claims 2 and 12 solely because it includes the word "installation." Moreover, while paragraph [0019] of Dahlstrom discusses tracking security vulnerabilities and corrective actions, there is no indication that such "tracking" is performed "in response to installation, configuration or maintenance of the computer system" as recited in Claims 2 and 12. As such, Claims 2, 8, 12 and 18 are independently patentable over the cited art.

C. Claims 3 and 13 are Separately Patentable Over the Cited Art

Claims 3 and 13 depend from Claims 1-2 and 11-12, respectively, and hence Claim 3 is patentable for each of the reasons that Claims 1 and 2 are patentable, and Claim 13 is patentable for each of the reasons that Claims 11 and 12 are patentable. In addition, Appellants submit that Claims 3 and 13 are independently patentable over the cited art. In particular, Claims 3 and 13 recite "updating a threat management information base for the computer system to account for the countermeasures that are processed." The Final Action cites to paragraphs [0027] and [0036] of Dahlstrom as disclosing the recitations of Claims 3 and 13. However, the cited portions of Dahlstrom relate to the updating of the product records **52**, which are what the Final Action alleges comprises the TMV as opposed to the threat management information base. (See Final Action at 2). As explained at pages 19-22 of the present specification, the threat management information base records a baseline vulnerability state of a target system, and hence the product records **52** of Dahlstrom – which list known vulnerabilities and fixes for specific products – clearly are not the "threat management information base" of Claims 3 and 13. Moreover, the "updating" discussed in paragraphs [0027] and [0036] of Dahlstrom does not have anything to do with "account[ing] for the countermeasures that are processed" as recited in Claims 3 and 13. Appellants note that the Final Action takes the position that it would be "inherent" that the countermeasures would have been processed at some point." (Final Action at 3). However, it is

not necessarily the case that the system of Dahlstrom would update a threat management information base for each organization's system to account for the processing of each countermeasure. Accordingly, the rejections of Claims 3 and 13 should be reversed.

D. Claims 4-5, 14-15 and 22 are Separately Patentable Over the Cited Art

Claims 4-5, 14-15 and 22 depend from one of Claims 1, 11 or 21, and hence each claim is patentable as depending from a patentable base claim. In addition, Appellants submit that Claims 4-5, 14-15 and 22 are independently patentable over the cited art. In particular, Claims 4-5, 14-15 and 22 each recite "adding at least one instance identifier to the TMV to account for multiple instances of the operating system running on the computer system, if the TMV identifies the operating system type and operating system release level for the computer system as being affected by the computer security threat." The Final Action cites to Col. 4, lines 26-37 of Flowers (Final Action at 4, 7) as disclosing this recitation, which recites:

A system and method in accordance with the invention reliably and non-intrusively identifies various conditions of a network. In particular, an embodiment of the invention can identify an operating system, including version and patch level, and a service, including version and patch level, of a remote host on the network. Using this information, an embodiment of the invention can then reliably identify a vulnerability condition of the network. In some embodiments, the operating system and service information can be used to identify a trojan application, unlicensed software use, security policy violations, or even infer vulnerabilities that are yet unknown.

This portion of Flowers simply has nothing to do with instance identifiers or accounting for multiple instances of an operating system running in the computer system. Accordingly, the rejections of Claims 4-5, 14-15, 17 and 22 should also be reversed for this additional reason.

E. Claims 6-7 and 16-17 are Separately Patentable Over the Cited Art

Claims 6 and 16 depend from Claims 1 and 11, respectively, and Claims 7 and 17 depend from Claims 6 and 16, respectively. Accordingly, each of Claims 6-7 and 16-17 is patentable as depending from a patentable base claim. In addition, Appellants submit that Claims 6-7 and 16-17 are independently patentable over the cited art. In particular, each of these claims recite

including fourth and fifth fields in a TMV that identify an application program type and a release level therefore. The Final Action again cites to Col. 4, lines 26-37 of Flowers as disclosing these recitations of Claims 6 and 16. However, the cited portion of Flowers discusses the output provided by the system of Flowers as opposed to a TMV. Thus, the Final Action takes the position that the product records 52 of Dahlstrom should be combined with the results provided by the system of Flowers (i.e., the identification of the operating system, including version and patch level) to allegedly arrive at a TMV according to embodiments of the present invention. Appellants respectfully submit that this combination does not make any sense, and that no motivation for such a combination exists. Accordingly, the rejections of Claims 6-7 and 16-17 should be reversed for this additional reason. Appellants note that the Response to Arguments section of the Final Action does not even attempt to rebut Appellants showing that Claims 6-7 and 16-17 are patentable over the cited art.

In addition, Claims 7 and 17 each include the same recitation of Claims 4, 14 and 22, discussed above, that is not found in the cited art. Accordingly, the rejections of Claims 7 and 17 should also be reversed for the same reasons, discussed above, that the rejections of Claims 4, 14 and 22 should be reversed.

F. Claims 9 and 19 are Separately Patentable Over the Cited Art

Claim 9 depends from Claim 1, and hence is patentable as depending from a patentable base claim. Claim 19 depends from Claims 11, 12 and 18, and hence is patentable for each of the reasons that Claims 11, 12 and 18 are patentable over the cited art. In addition, Appellants submit that Claims 9 and 19 are independently patentable over the cited art. In particular, Claims 9 and 19 recite pruning a TMV to discard at least some of the TMV that is not needed for processing countermeasures. The Final Action cites to Dahlstrom at paragraph [0027] as disclosing the recitations of Claims 9 and 19, and argues that the "updates" described therein would inherently include "discard[ing] old information and replacing it with new information." (Final Action at 4 and 9). Appellants respectfully submit, however, that (1) product records can

clearly be updated without discarding information (and hence the Final Action fails to establish inherency) and (2) that it is not inherent that the information that is pruned is information "that is not needed for processing countermeasures" as recited in Claims 9 and 19. Accordingly, the rejections of Claims 9 and 19 should be reversed for this additional reason.

G. Claims 10 and 20 are Separately Patentable Over the Cited Art

Claims 10 and 20 depend from Claims 1 and 11, respectively, and hence each claim is patentable as depending from a patentable base claim. In addition, Appellants submit that Claims 10 and 20 are independently patentable over the cited art. In particular, Claims 10 and 20 recite mutating a TMV to a format that is compatible with processing countermeasures. The Final Action cites to paragraph [0042] of Dahlstrom as disclosing the recitations of Claims 10 and 20, but the cited passage simply does not disclose or suggest the claimed subject matter. Instead, paragraph [0042] of Dahlstrom discusses the information contained in the organization profile 72. This organization profile is not a TMV, nor does Dahlstrom describe mutating the profile to a format that is compatible with processing countermeasures. Accordingly, the rejections of Claims 10 and 20 should also be reversed.

In re: Bardsley et al.
Serial No.: 10/624,158
Filed: July 22, 2003
Page 13

II. Conclusion

In light of the above, Appellants submit that each of the pending claims is patentable over the cited references and, therefore, request reversal of the rejections of Claims 1-22.

Respectfully submitted,

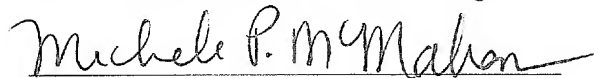


D. Randal Ayers
Registration No. 40,493
Attorney for Appellants

Customer Number 20792
Myers Bigel Sibley & Sajovec, P.A.
P.O. Box 37428
Raleigh, NC 27627
919-854-1400
919-854-1401 (Fax)

CERTIFICATION OF TRANSMISSION

I hereby certify that this correspondence is being transmitted via the Office electronic filing system in accordance with § 1.6(a)(4) to the U.S. Patent and Trademark Office on August 17, 2007.


Michele P. McMahan

CLAIMS APPENDIX
Pending Claims USSN 10/624,158
Filed July 22, 2003

1. A method of administering a countermeasure for a computer security threat to a computer system, comprising:

establishing a baseline identification of an operating system type and an operating system release level for the computer system that is compatible with a Threat Management Vector (TMV);

receiving a TMV including therein a first field that provides identification of at least one operating system type that is affected by a computer security threat, a second field that provides identification of an operating system release level for the operating system type and a third field that provides identification of a set of possible countermeasures for an operating system type and an operating system release level; and

processing countermeasures that are identified in the TMV if the TMV identifies the operating system type and operating system release level for the computer system as being affected by the computer security threat.

2. A method according to Claim 1:

wherein the receiving comprises receiving a TMV history file in response to installation, configuration or maintenance of the computer system; and

wherein the processing comprises processing countermeasures that are identified in the TMV history file.

3. A method according to Claim 2 further comprising updating a threat management information base for the computer system to account for the countermeasures that are processed.

4. A method according to Claim 1 wherein the processing comprises:

determining whether the TMV identifies the operating system type and operating system release level for the computer system as being affected by the computer security threat;

adding at least one instance identifier to the TMV to account for multiple instances of the operating system running on the computer system, if the TMV identifies the operating system type and operating system release level for the computer system as being affected by the computer security threat; and

processing countermeasures that are identified in the TMV for the instance of the operating system type and operating system release level when the instance of the operating system type and operating system release level is instantiated in the computer system.

5. A method according to Claim 4 wherein the processing comprises installing and running the countermeasure.

6. A method according to Claim 1:

wherein the receiving comprises receiving a TMV including therein the first field that provides identification of at least one operating system type that is affected by a computer security threat, the second field that provides identification of an operating system release level for the operating system type, a fourth field that provides identification of at least one application program type that is affected by the computer security threat and a fifth field that provides identification of a release level for the application program type, the third field providing identification of a set of possible countermeasures for the application program type and the application program release level; and

wherein the processing comprises processing countermeasures that are identified in the TMV if the TMV identifies the application program type and application program release level for the computer system as being affected by the computer security threat.

7. A method according to Claim 6 wherein the processing further comprises:

determining whether the TMV identifies the application program type and application programming release level for the computer system as being affected by the computer security threat;

adding at least one instance identifier to the TMV to account for multiple instances of the application program running on the computer system if the TMV identifies the application program type and application program release level for the computer system as being affected by the computer security threat; and

processing countermeasures that are identified in the TMV for the instance of the application program type and application program release level when the instance of the application program type and application program release level is instantiated in the computer system.

8. A method according to Claim 2 wherein the set of possible countermeasures comprises an identification of a countermeasure mode of installation.

9. A method according to Claim 1 wherein the receiving comprises pruning at least some of the TMV to discard at least some of the TMV that is not needed for processing countermeasures.

10. A method according to Claim 1 wherein the receiving comprises mutating the TMV that is received to a format that is compatible with processing countermeasures.

11. A computer system, comprising:
a Threat Management Information Base (TMIB) that is configured to establish a baseline identification of an operating system type and an operating system release level for the computer system that is compatible with a Threat Management Vector (TMV);
a TMV receiver that is configured to receive a TMV including therein a first field that

provides identification of at least one operating system type that is affected by a computer security threat, a second field that provides identification of an operating system release level for the operating system type and a third field that provides identification of a set of possible countermeasures for an operating system type and an operating system release level; and

a remediation manager that is configured to process countermeasures that are identified in the TMV if the TMV identifies the operating system type and operating system release level for the computer system as being affected by the computer security threat.

12. A system according to Claim 11 further comprising:

a TMIB configurator that is configured to receive a TMV history file in response to installation, configuration or maintenance of the computer system and to process countermeasures that are identified in the TMV history file.

13. A system according to Claim 12 wherein the TMIB configurator is further configured to update the TMIB to account for the countermeasures that are processed.

14. A system according to Claim 11 further comprising:

a TMV inductor that is configured to determine whether the TMV identifies the operating system type and operating system release level for the computer system as being affected by the computer security threat and to add at least one instance identifier to the TMV to account for multiple instances of the operating system running on the computer system, if the TMV identifies the operating system type and operating system release level for the computer system as being affected by the computer security threat; and

wherein the remediation manager is further configured to process countermeasures that are identified in the TMV for the instance of the operating system type and operating system release level when the instance of the operating system type and operating system release level is instantiated in the computer system.

15. A system according to Claim 14 wherein the remediation manager is configured to process countermeasures that are identified in the TMV by installing and running the countermeasure.

16. A system according to Claim 11:
wherein the TMV receiver is further configured to receive a TMV including therein the first field that provides identification of at least one operating system type that is affected by a computer security threat, the second field that provides identification of an operating system release level for the operating system type, a fourth field that provides identification of at least one application program type that is affected by the computer security threat and a fifth field that provides identification of a release level for the application program type, the third field providing identification of a set of possible countermeasures for the application program type and the application program release level; and

wherein the remediation manager is further configured to process countermeasures that are identified in the TMV if the TMV identifies the application program type and application program release level for the computer system as being affected by the computer security threat.

17. A system according to Claim 16 further comprising:
a TMV inductor that is configured to determine whether the TMV identifies the application program type and application programming release level for the computer system as being affected by the computer security threat and to add at least one instance identifier to the TMV to account for multiple instances of the application program running on the computer system if the TMV identifies the application program type and application program release level for the computer system as being affected by the computer security threat; and

wherein the remediation manager is further configured to process countermeasures that are identified in the TMV for the instance of the application program type and application

program release level when the instance of the application program type and application program release level is instantiated in the computer system.

18. A system according to Claim 12 wherein the set of possible countermeasures comprises an identification of a countermeasure mode of installation.

19. A system according to Claim 18 wherein the TMV receiver is further configured to prune at least some of the TMV that is not needed by the remediation manager.

20. A system according to Claim 11 wherein the TMV receiver is further configured to mutate the received TMV to a format that is compatible with the remediation manager.

21. A computer program product is configured to administer a countermeasure for a computer security threat to a computer system, the computer program product comprising a computer usable storage medium having computer-readable program code embodied in the medium, the computer-readable program code comprising:

computer-readable program code that is configured to establish a baseline identification of an operating system type and an operating system release level for the computer system that is compatible with a Threat Management Vector (TMV);

computer-readable program code that is configured to receive a TMV including therein a first field that provides identification of at least one operating system type that is affected by a computer security threat, a second field that provides identification of an operating system release level for the operating system type and a third field that provides identification of a set of possible countermeasures for an operating system type and an operating system release level; and

computer-readable program code that is configured to process countermeasures that are identified in the TMV if the TMV identifies the operating system type and operating system release level for the computer system as being affected by the computer security threat.

22. A computer program product according to Claim 21 wherein the computer-readable program code that is configured to process comprises:

computer-readable program code that is configured to determine whether the TMV identifies the operating system type and operating system release level for the computer system as being affected by the computer security threat;

computer-readable program code that is configured to add at least one instance identifier to the TMV to account for multiple instances of the operating system running on the computer system if the TMV identifies the operating system type and operating system release level for the computer system as being affected by the computer security threat; and

computer-readable program code that is configured to process countermeasures that are identified in the TMV for the instance of the operating system type and operating system release level when the instance of the operating system type and operating system release level is instantiated in the computer system.

In re: Bardsley et al.
Serial No.: 10/624,158
Filed: July 22, 2003
Page 21

EVIDENCE APPENDIX

No evidence is being submitted with this *Appeal Brief* pursuant to 37 C.F.R. §§ 1.130, 1.131 or 1.132.

RELATED PROCEEDINGS APPENDIX

The subject matter of the present application is related to U.S. Application Serial No. 10/624,344 (although not by a claim of priority). U.S. Application Serial No. 10/624,344 is currently in prosecution, and Appellants have appealed the rejections of the claims in that application to the Board of Patent Appeals and Interferences via a Notice of Appeal filed December 21, 2006 and an Appeal Brief filed February 2, 2007. No decision has been rendered in this appeal as of the date of this Appeal Brief.